

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of:

**COMMUNICATIONS ASSISTANCE FOR LAW
ENFORCEMENT ACT**

RM-10865

Joint Petition for Expedited Rulemaking, filed by
United States Department of Justice, Federal
Bureau of Investigation and Drug Enforcement
Administration

To: Office of Engineering and Technology

REPLY COMMENTS OF LEVEL 3 COMMUNICATIONS, LLC

Greg L. Rogers
LEVEL 3 COMMUNICATIONS, LLC
1025 Eldorado Boulevard
Broomfield, CO 80021
Tel: (720) 888-2512
Fax: (720) 888-5134

Stewart A. Baker
Chung Hsiang Mah
Michael T. Gershberg
STEPTOE & JOHNSON LLP
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036
Tel: (202) 429-3000
Fax: (202) 429-3902
Counsel for Level 3 Communications, LLC

April 27, 2004

TABLE OF CONTENTS

I.	SCOPE OF CALEA.....	- 2 -
II.	ENFORCING COMPLIANCE WITH CALEA.....	- 4 -
	A. Enforcement Measures for Existing Providers of Packet-Mode Services	- 5 -
	B. Enforcement Measures for Future Services	- 6 -
III.	COST RECOVERY ISSUES	- 8 -
IV.	CONCLUSION.....	- 11 -

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of:

**COMMUNICATIONS ASSISTANCE FOR LAW
ENFORCEMENT ACT**

RM-10865

Joint Petition for Expedited Rulemaking, filed by
United States Department of Justice, Federal
Bureau of Investigation and Drug Enforcement
Administration

To: Office of Engineering and Technology

REPLY COMMENTS OF LEVEL 3 COMMUNICATIONS, LLC

I. INTRODUCTION

Level 3 Communications, LLC (“Level 3”) hereby submits these reply comments on the Joint Petition for Expedited Rulemaking (“Petition”) filed by the United States Department of Justice, Federal Bureau of Investigation, and Drug Enforcement Administration (“Law Enforcement”). The Petition requests the Commission to (1) rule on the scope of the Communications Assistance for Law Enforcement Act (“CALEA”); (2) issue rules for enforcing compliance with CALEA for both existing and new services; and (3) make certain declarations regarding cost recovery for compliance with CALEA.

Level 3 recognizes the important interests of Law Enforcement in being able to conduct electronic surveillance for the investigation and prevention of crime, including terrorism. In fact, Level 3 is a firm supporter of such interests and has devoted substantial resources to assisting Law Enforcement with lawful surveillance requests. It has also made great advances toward bringing its services into full CALEA compliance without protracted debate about whether it is

legally required to do so. However, Level 3 is concerned that the Petition overreaches in certain respects and that some of the outcomes sought by Law Enforcement are beyond the scope of the statute or would not serve the public interest.

I. SCOPE OF CALEA

CALEA expressly applies only to “telecommunications carriers” and not “information services.” This is clear from both the statutory text,¹ the legislative history,² and Commission orders.³ Congress deliberately excluded information services from the scope of CALEA in order to protect personal privacy and to preserve innovation.⁴ Nevertheless, the Petition requests a declaratory ruling by the Commission that “broadband access service” and “broadband telephony” are subject to CALEA.⁵ But many forms of broadband access service and broadband

¹ 47 U.S.C. § 1001(8)(c)(i) (excluding providers of information services from the definition of “telecommunications carrier”); 47 U.S.C. § 1002(b)(2) (providing that the intercept capabilities in § 1002(a) do not apply to information services).

² See H.R. Rep. No. 103-827, 1994 U.S.C.C.A.N. 3489, 3503 (1994) (“*Legislative History*”) (CALEA’s obligations “do not apply to information services, such as electronic mail services, or on-line services, such as Compuserve, Prodigy, America-On-line or Mead Data, or Internet service providers.”).

³ See *Second Report and Order*, 15 FCC Rcd 7105, ¶ 27 (1999).

⁴ See *Legislative History* at 3493 (“Therefore, the bill seeks to balance three key policies: (1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies.”); *id.* at 3498 (“It is also important from a privacy standpoint to recognize that the scope of the legislation has been greatly narrowed. The only entities required to comply with the functional requirements are telecommunications common carriers . . .”); *id.* at 3501 (“It is the Committee’s intention not to limit the definition of “information services” to such current services, but rather to anticipate the rapid development of advanced software and to include such software services in the definition of “information services.” By including such software-based electronic messaging services within the definition of information services, they are excluded from compliance with the requirements of the bill.”).

⁵ See Petition 15-32.

telephony are likely to be “information services”⁶ exempt from CALEA. Because the intercept capability requirements of CALEA expressly “do not apply to . . . information services,”⁷ the Petition overreaches to the extent it seeks to subject such services to CALEA.

In Level 3’s view, CALEA applies only to carrier-level packet transport services and was never intended to cover a myriad of higher-level information services. The exemption of information services recognizes the practical limitations of attempting to regulate services that are not readily defined or recognizable. It is often impossible for the carrier providing the packet transport services to know what information services are being provided over its network. Information services tend to come in many different varieties and tend to evolve rapidly. Such services are often provided by third party providers with whom the carrier may have no relationship. Moreover, the call-identification-like information used to provide information services is often encapsulated within several layers of packets using protocols unfamiliar to the carrier. And, of course, the information may also be encrypted. All of this can make it very difficult for the carrier to be able to extract relevant information from such higher-level services.

Given these difficulties, CALEA obligations should only be imposed on telecommunications carriers consistent with the Commission’s precedent rather than making a quixotic attempt to expand the reach of the Commission. This becomes particularly evident when one considers that CALEA does not expand or contract law enforcement’s legal authority

⁶ See *Appropriate Framework for Broadband Access to the Internet over Wireline Facilities*, Notice of Proposed Rulemaking, 17 FCC Rcd 3019, 3029 ¶ 17 (2002) (wireline broadband service); *In the Matter of Inquiry Concerning High-Speed Access to the Internet over Cable and Other Facilities*, Declaratory Ruling and Notice of Proposed Rulemaking, 17 FCC Rcd 4798, 4802 ¶ 7 (2002) (cable broadband service); *In the Matter of Petition for Declaratory Ruling that pulver.com’s Free World Dialup is Neither Telecommunications Nor a Telecommunications Service*, Memorandum Opinion and Order, FCC 04-27, WC Docket No. 03-45, ¶¶ 1-2 (Feb. 19, 2004) (broadband telephony).

⁷ 47 U.S.C. § 1002(b)(2).

no matter how it is imposed. Level 3 is committed to supporting law enforcement efforts to maintain effective tools to protect the public. However, the Petition's attempt to sweep prior precedent aside and embark upon a regulatory framework destined to fail is inadvisable. The Commission does not need to abandon its definitions of "telecommunications" and "information services" to effectively require carriers to support legal intercept capabilities that are technically feasible.

II. ENFORCING COMPLIANCE WITH CALEA

CALEA itself sets out the means for ensuring compliance with its requirements. Indeed, Congress was very careful in its choice of means and institutions for enforcing CALEA. In particular, it committed primary enforcement responsibility to the courts and reserved only a limited role for the Commission.⁸

Nevertheless, the Petition asks the Commission to impose extensive new measures to enforce compliance with CALEA for both existing providers of packet-mode services and for new packet-mode services. For existing providers, the Petition proposes a series of implementation milestones backed by Commission enforcement action.⁹ For future services, the

⁸ Section 108 of CALEA explicitly gives responsibility for CALEA enforcement to the federal courts. This enforcement authority may be exercised only if the court finds that "alternative technologies or capabilities or the facilities of another carrier are not reasonably available to law enforcement for implementing the interception" and "compliance with the requirements of [CALEA] is reasonably achievable." 47 U.S.C. § 1007(a). The Commission, on the other hand, has authority to act only in certain areas that do not include enforcement. *See* 47 U.S.C. §§ 1001(8), 1004, 1006(b)-(c), 1008(b)(1). Furthermore, the Commission's general rulemaking authority to implement CALEA under Section 229 of the Communications Act of 1934 does not empower the Commission to alter the express requirements of CALEA. The courts have rejected arguments that an agency "possesses *plenary* authority to act within a given area simply because Congress has endowed it with *some* authority to act in that area." *Railway Labor Executives' Ass'n v. National Mediation Bd.*, 29 F.3d 655, 670 (D.C. Cir. 1994) (en banc).

⁹ *See* Petition at 34-53.

Petition proposes to presume new services to be covered by CALEA.¹⁰ Under this presumption, the provider of a new service must either build CALEA capability into its system before deploying its service, or else petition the Commission for a ruling that the service is not covered.¹¹

A. Enforcement Measures for Existing Providers of Packet-Mode Services

Because Level 3 is aggressively implementing CALEA-compliant capabilities irrespective of service categories, Level 3 leaves to others the argument whether the Commission has any legal authority to impose CALEA requirements on existing packet-mode services or to impose the proposed enforcement measures. However, Level 3 cautions against a rush to extend the law when it is not clear that an extension is necessary. Law enforcement already has ample legal tools under Title III of the Omnibus Safe Streets and Crime Control Act of 1968 (“Title III”)¹² and the Electronic Communications Privacy Act (“ECPA”)¹³ for the conduct of lawful intercepts, and there is no evidence that industry has not cooperated in the execution of lawful intercept orders.¹⁴

In addition, there have been extensive voluntary efforts by industry to bring their networks into compliance with the CALEA requirements for packet-mode technologies. While

¹⁰ *See id.* at 53-57.

¹¹ *Id.* at 53-54.

¹² Pub. L. No. 90-351, 82 Stat. 212 (1968) (codified, as amended at 18 U.S.C. §§ 2510 *et seq.*).

¹³ Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified, as amended at 18 U.S.C. §§ 2701 *et seq.*, 3121 *et seq.*).

¹⁴ Level 3 has an excellent record in complying with lawfully authorized intercept requests. *See Level 3 Petition for Extension of CALEA Compliance Deadline* (filed Jan. 30, 2004) (“*Level 3 Petition*”) (filed under seal).

Level 3 cannot speak for other carriers, Level 3 is very close to being able to deploy a CALEA-compliant intercept solution across its entire network. Level 3 expects that its solution will be in place by the end of 2004.¹⁵ There is reason to think that other major carriers, such as the Regional Bell Operating Companies (“RBOCs”), may be similarly situated. The RBOCs are notably absent from the list of carriers requesting extensions of their CALEA compliance deadlines referred to in the Petition as examples of the lack of implementation of packet-mode intercept capabilities.¹⁶ This suggests that, like Level 3, the RBOCs and other major carriers may have already implemented or may be very close to implementing CALEA functionality for their packet transport services.

If so, the aggressive implementation plan of the kind proposed in the Petition may be unnecessary. While significant technological challenges remain, it would appear that in a short while the voluntary implementation of packet-mode CALEA capabilities by the carriers that serve the vast majority of people in the United States will be in place. With that said, Level 3 would not object to a reasonable compliance schedule that recognizes the undisputed technical hurdles that must be overcome to support law enforcement’s requests in an Internet Protocol environment.

B. Enforcement Measures for Future Services

For future services, the Petition proposes the adoption of “rules requiring that a carrier already have installed and deployed a CALEA solution . . . at the time the carrier rolls out that CALEA-covered service to the public”¹⁷ The Petition goes on to state that if “a carrier

¹⁵ *See Id.*

¹⁶ Petition at 35-36 nn. 62-63.

¹⁷ Petition at 54.

plans to begin offering a new service and is unsure whether that service is subject to CALEA, the Commission should require the carrier to file a request for a clarification or declaratory ruling that seeks Commission guidance on CALEA's applicability to the proposed service offering.”¹⁸

Such measures are directly inconsistent with one of the “key policies” of CALEA, which is “to avoid impeding the development of new communications services and technologies.”¹⁹ This goal is codified throughout CALEA. For example, CALEA specifically prevents Law Enforcement from requiring specific system designs and from prohibiting the adoption of any service.²⁰ Also, companies may even deploy inaccessible technologies without being subject to a CALEA compliance suit if compliance is not “reasonably achievable through the application of available technology to the equipment.”²¹ It would impede innovation and distort competition to presume that new technologies are covered by CALEA, or to require that the Commission give its permission before a technology is deployed.

First, such a presumption would raise the cost of market entry for new communications technologies and services. Because of the extra time and costs of designing and building CALEA capabilities into new services even before their success in the market is known, pioneering and potentially valuable new technologies may never be deployed or may only be marketable much later by a select few companies capable of withstanding such heavy regulation.

Second, even if a company were to seek a declaration from the Commission that its new service was not covered by CALEA, it would have to disclose its new technology before it is

¹⁸ *Id.*

¹⁹ *Legislative History* at 3493.

²⁰ 47 U.S.C. § 1002(b)(1)(A)-(B).

²¹ 47 U.S.C. § 1007(a)(2).

deployed. This would give the company's rivals the opportunity to preview the new technology and the incentive to either block its introduction or to prepare for its arrival.

Together, such rules are likely to have a substantial and lasting effect on the rate of innovation in communications technologies and services – a result completely contrary to one of the key policies of CALEA, which is to avoid impeding technological innovation. Indeed, Congress specifically rejected earlier versions of CALEA which would have shackled new technologies with intercept capability requirements.²²

Finally, it must be acknowledged that as a purely practical matter it is impossible to guarantee that any and all potential technological applications are capable of being effectively regulated. What Law Enforcement is essentially asking the Commission to do, when it requests that the Commission make CALEA “future proof,” is to knowingly implement unenforceable rules. The Petition's proposal for future services is not based upon sound legal or public policy grounds and should therefore be rejected by the Commission.

III. COST RECOVERY ISSUES

The Petition requests the Commission to (i) declare that carriers bear sole responsibility for CALEA implementation cost after January 1, 1995; (ii) permit carriers to recover implementation costs from their customers; and (iii) “clarify” that carriers cannot include CALEA implementation costs in their administrative intercept provisioning charges to Law Enforcement.²³ The Commission should decline to make these declarations for three reasons.

²² See *Legislative History* at 3499 (“The bill expressly provides that law enforcement may not dictate system design features and may not bar introduction of new features and technologies. . . . This is the exact opposite of the original versions of the legislation, which would have barred introduction of services or features that could not be tapped.”).

²³ Petition at 63-70.

First, the Petition overreaches to the extent that it claims that carriers must bear *all* of the costs of implementing CALEA solutions for post-January 1, 1995 equipment, facilities and services. CALEA itself provides a mechanism whereby a carrier can petition the Commission for a declaration that compliance with CALEA is not “reasonably achievable,” and then, if successful, to request compensation from the Attorney General for complying with CALEA. If the Attorney General does not agree to pay, the carrier is then deemed to be in compliance with the statute’s requirements. Reasonable achievability is to be judged on a number of criteria, including: (a) the effect on rates for basic residential telephone service;²⁴ (b) the effect on the nature, cost and operation of the equipment, facilities and services at issue;²⁵ (c) the policy of the United States to encourage the provision of new technologies and services to the public;²⁶ (d) the financial resources of the telecommunications carrier;²⁷ and (e) the effect on competition in the provision of telecommunications services.²⁸ This statutory provision cannot be overridden by the Commission.

Second, many cost recovery mechanisms for lawfully authorized electronic surveillance are not in the Communications Act or CALEA. For example, the provisions for recovering the costs of wiretap orders are contained in other federal and state statutes which, typically, commit authority over cost recovery to the court issuing the order.²⁹ There is nothing to suggest that the

²⁴ 47 U.S.C. § 1008(b)(1)(B).

²⁵ 47 U.S.C. § 1008(b)(1)(E)-(F).

²⁶ 47 U.S.C. § 1008(b)(1)(G).

²⁷ 47 U.S.C. § 1008(b)(1)(H).

²⁸ 47 U.S.C. § 1008(b)(1)(I).

²⁹ *See, e.g.*, 18 U.S.C. §§ 2518(4), 2706, 3124(c).

Commission has any authority to pronounce on the scope of recovery under those statutory provisions. But even assuming that it did, the Commission has already ruled that carriers may recover “a portion of their CALEA software and hardware costs by charging to [law enforcement agencies], for each electronic surveillance order authorized by CALEA, a fee that includes recovery of capital costs, as well as recovery of the specific costs associated with each order.”³⁰ This more contemporaneous interpretation of CALEA cannot be overturned without a “reasoned analysis” explaining why the Commission is changing course.³¹ There is no basis here for departing from the Commission’s prior decision.

Finally, security from crime and terrorism is a classic public good. Its benefits accrue to all of society, and certainly not just to communications carriers and their respective customers. On this basis, the costs of CALEA compliance are better borne by the public purse. In this case, this means that such costs should be borne by law enforcement and ultimately by citizens at large. Indeed, failure to place the cost burden on law enforcement (the intended user of CALEA capabilities) would have at least two undesirable effects on the allocation of resources: (a) law enforcement would have every incentive to demand costly intercept capabilities, even those that cannot be justified by the likely investigative benefits; and (b) law enforcement would have no incentive to develop less costly investigative tools in place of costly wiretaps and other CALEA capabilities. It thus makes no sense to impose these costs on carriers and their customers alone.

³⁰ *In the Matter of Communications Assistance for Law Enforcement Act*, Order on Remand, CC Docket No. 97-213, 17 FCC Rcd 6896, 6917 ¶ 60 (April 5, 2002).

³¹ *See Motor Vehicle Manufacturers Ass’n of the U.S., Inc. v. State Farm Mutual Automobile Insurance Co.*, 463 U.S. 29, 42 (1983) (“[A]n agency changing its course . . . is obligated to supply a reasoned analysis for the change”); *Greater Boston Television Corp. v. FCC*, 444 F.2d 841, 852 (D.C. Cir. 1970) (“[A]n agency changing its course must supply a reasoned analysis indicating that prior policies and standards are being deliberately changed, not casually ignored, and if an agency glosses over or swerves from prior precedents without discussion it may cross the line from the tolerably terse to the intolerably mute.”).

Instead, the public interest would be better served by requiring law enforcement to pay their fair share of the costs of implementing CALEA.

IV. CONCLUSION

Level 3 continues to strongly support the important social policy of ensuring that law enforcement continues to have the ability to conduct lawfully authorized electronic surveillance. However, in pursuing this goal, the Commission should avoid impeding technological innovation in communications services and technologies and ensure that law enforcement bears its fair share of the costs of providing such capabilities. Accordingly, the Commission should not adopt all of the measures in the Petition because of their distortive effect on innovation, competition and resource allocation.

Respectfully submitted,



Greg L. Rogers
LEVEL 3 COMMUNICATIONS, LLC
1025 Eldorado Boulevard
Broomfield, CO 80021
Tel: (720) 888-2512
Fax: (720) 888-5134

Stewart A. Baker
Chung Hsiang Mah
Michael T. Gershberg
STEPTOE & JOHNSON LLP
1330 Connecticut Avenue NW
Washington, DC 20036
Tel: (202) 429-3000
Fax: (202) 429-3902

Counsel for Level 3 Communications, LLC

April 27, 2004